Devoir surveillé $n°01$
Correction

N'hésitez pas de me signaler les erreurs rencontrées.

•••••••••

-Première partie-

1. Les éléments inversibles de $\mathbf{Z}/6\mathbf{Z}$ sont $1, 5$ qui sont leurs propres inverses. Par contre tous les éléments non nuls de $\mathbf{Z}/13\mathbf{Z}$ sont inversibles (13 est premier).
2. Déjà p doit être impair. Donc $p \equiv -1, 1$ ou 3 modulo 6 (6 est pair !). Si $p \equiv 3\ [6]$ alors $3 \mid p$. C'est possible pour $p = 3, p + 2 = 5$ mais ces solutions sont exclues par l'énoncé.
   De même, si on avait $p \equiv 1\ [6]$ alors $3 \mid p + 2$ ce qui est possible mais seulement avec $p = 1$, exclus. Reste la seule possibilité que $p \equiv -1\ [6]$.
3. Un polynôme de degré deux est irréductible $\iff$ il n'a pas de factorisation non triviale $\iff$ il n'a pas de racine ! Or $\overline{5}$ n'est pas un carré dans $\mathbf{Z}/13\mathbf{Z}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1

   Les carrés sont donc $0, 1, 4, 9, 3, 12, 10$ et par conséquent $X^2 - \overline{5}$ est irréductible dans $\mathbf{Z}/13\mathbf{Z}[X]$.

-Deuxième partie-

1. Il est clair que la loi est interne et associative (est dans un anneau), par ailleurs le produit de a, b inversibles est encore inversible, d'inverse le produit des inverses, et l'inverse d'un élément inversible est bien évidemment inversible. On a vérifié les quatre axiomes d'un groupe.
2. $\overline{a}$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$ $\iff$ il existe $\exists \overline{u} \in \mathbf{Z}/n\mathbf{Z} \mid \overline{a}.\overline{u} = \overline{1}$ $\iff$ $\exists u \in \mathbf{Z} \mid au \equiv 1\ [n]$ $\iff$ $\exists (u, v) \in \mathbf{Z}^2 \mid au = 1 + vn$.
   Et là on reconnaît la propriété de Bezout, qui équivaut à $a \wedge n = 1$. On a montré que $\mathbf{U}(\mathbf{Z}/n\mathbf{Z}) = V$.
3. Soit $\overline{a} \in, \mathbf{Z}/n\mathbf{Z} \setminus \{\overline{0}\}$.
$$\exists \overline{b} \neq 0 \mid \overline{a}.\overline{b} = 0 \iff \exists b \notin n\mathbf{Z}, \exists k \in \mathbf{Z} \mid ab = kn$$
   Si a était premier avec n, par le théorème de Gauss n, qui divise ab, diviserait b ce qui est absurde. On trouve donc que a et n ont un facteur commun $d > 1$. Réciproquement, si $a \wedge n = d > 1$ alors pour $b = \dfrac{n}{d}$ on a bien
$$\overline{b} \neq 0 \qquad \overline{a}.\overline{b} = \overline{ab} = \overline{0}$$
   Donc l'ensemble des diviseurs de $\overline{0}$ est bien D.

-Troisième partie-

1. Il est clair que que $(\mathbf{K}_{13}, \oplus)$ est un groupe additif, car c'est le produit de deux groupes (groupe produit) et que la loi $\bullet$ est une loi de composition interne, mais il faut vérifier qu'elle est associative. D'autre part, il est évident qu'elle est commutative.
   Ensuite cette loi $\bullet$ admet un élément neutre, $\mathbf{1} = (\overline{1}, \overline{0})$, et on vérifie aussi que $\bullet$ est **distributive** par rapport à $\oplus$. À ce stade, on a montré que $\mathbf{K}_{13}$ est un anneau commutatif.
   Reste donc à prouver que $\mathbf{K}_{13}$ est un corps. Soit donc $(x, y) \neq (\overline{0}, \overline{0})$ et cherchons (x', y') solution du système :
$$\begin{cases} xx' + \overline{5}yy' & = \overline{1} \\ xy' + yx' & = \overline{0}. \end{cases}$$

En multipliant par y la première équation, il vient $y = xx'y + \overline{5}y^2y' = \overline{5}y^2y' - x^2y' = -y'(x^2 - \overline{5}y^2)$. De même on trouve $x = x'(x^2 - \overline{5}y^2)$.
∘ Si $y = \overline{0}$ il n'y a pas de difficulté, on obtient $y' = \overline{0}, x' = x^{-1}$.
∘ Si $y \neq \overline{0}$, alors $x^2 - \overline{5}y^2$ n'est jamais nul. Sinon xy^{-1} serait une racine du polynôme $X^2 - \overline{5}$ et il n'y en a pas, d'après la question **3.** de la première partie. Or un élément non nul de $\mathbf{Z}/13\mathbf{Z}$ y admet un inverse.
On peut donc résoudre :

$$x' = (x^2 - \overline{5}y^2)^{-1}x \quad \text{et} \quad y' = -(x^2 - \overline{5}y^2)^{-1}y.$$

On a montré que $\mathbf{K}_{13}$ est un corps. Comme ensemble c'est $(\mathbf{Z}/13\mathbf{Z})^2$, il a donc 169 éléments.

2. Si $(x, \overline{0})$ et $(y, \overline{0})$ sont dans H_{13}, alors :

$$\begin{aligned}(x, \overline{0}) - (y, \overline{0}) &= (x - y, \overline{0}) \\ (x, \overline{0}) \bullet (y, \overline{0}) &= (xy, \overline{0})\end{aligned}$$

ce qui prouve que $(x, \overline{0}) - (y, \overline{0})$ et $(x, \overline{0}) \bullet (y, \overline{0})$ sont dans H_{13}. D'autre part, si $(x, \overline{0}) \neq (0, \overline{0})$, alors

$$(x, \overline{0})^{-1} = (x^{-1}, \overline{0}) \in H_{13}.$$

Finalement, on a bien prouvé que $(H_{13}, \oplus, \bullet)$ est un sous-corps de $(K_{13}, \oplus, \bullet)$. D'autre part l'application

$$\begin{array}{rccc}\Phi : & H_{13} & \to & \mathbf{Z}/13\mathbf{Z} \\ & (x, \overline{0}) & \mapsto & x\end{array}$$

est un morphisme d'anneaux bijectif. Donc les deux corps $(H_{13}, \oplus, \bullet)$ et $(\mathbf{Z}/13\mathbf{Z}, +, .)$ sont isomorphes.

3. Posons $\alpha = (x, y)$, il vient $\alpha^2 = (x^2 + \overline{5}y^2, 2xy) = (\overline{5}, \overline{0})$. On a donc $xy = \overline{0}$ et cela conduit rapidement aux deux solutions $\alpha = (\overline{0}, \overline{1})$ ou $\beta = (\overline{0}, -\overline{1}) = -\alpha$.
Dans $\mathbf{K}_{13}[X]$ on peut donc écrire

$$X^2 - \overline{5} = (X - (\overline{0}, \overline{1}))(X + (\overline{0}, \overline{1})) = (X - \alpha)(X + \alpha)$$

-Quatrième partie-

1. Soit $r \in \mathbf{N}$ tel que $(x^{-1})^r = e$ (en notant e l'élément neutre de G). Alors on a $x^{-r} = e$ et donc $x^r = e$. Donc l'ordre de x divise celui de x^{-1}. Et vice versa, donc $o(x^{-1}) = o(x)$.

2. Notons d l'ordre de ab. Remarquons que $(ab)^{mn} = (a)^m(b)^n = e$, et donc d divise mn. De plus, puisque $(ab)^d = e$, on en déduit que $a^d = b^{-d}$. il vient alors

$$a^{dn} = (b^{-d})^n = (b^n)^{-d} = e.$$

Ainsi, m divise dn et puisque m et n sont premiers entre eux, on en déduit que dn. De la même façon, on a md et en utilisant à nouveau que m et n sont premiers entre eux, on conclut que mn divise d. Ainsi, on a bien que $d = mn$.

3. On va essayer de se ramener au cas précédent. Si $d = m \wedge n$ on pose $m' = \dfrac{m}{d}, n' = n$ et on a $m' \wedge n' = 1$ et $m' \vee n' = m \vee n = m'n'$.
On pose alors $a' = a^d$, l'ordre de a' est $o(a') = \dfrac{o(a)}{d} = \dfrac{m}{d} = m'$.
D'après la question précédente, on a $o(a'b) = m'n = m \vee n$. Donc il suffit de prendre $c = ab$.

4. On note m le ppcm des ordres des éléments de $(G, .)$ et l'on introduit sa décomposition en facteurs premiers

$$m = p_1^{\alpha_1} ... p_N^{\alpha_N}.$$

Puisque $p_i^{\alpha_i}$ est facteur du ppcm des ordres des éléments de $(G, .)$, il existe un élément y_i dans G d'ordre $p_i^{\alpha_i}d$ pour un certain $d \in \mathbf{N}^*$. L'élément $x_i = y_i^d$ est alors d'ordre exactement $p_i^{\alpha_i}$.
D'après la question précédente, l'élément $y = x_1 ... x_m$ est d'ordre m.

5. Soit r l'exposant de G : tout élément de G vérifie donc $x^r = 1$. Mais cette équation, dans F, possède **au plus** r **racines distinctes** d'après le résultat suivant :

Si F est un corps, un polynôme $P \in F[X]$ de degré d a au plus d racines dans F.

qui se démontre par récurrence sur d (divisant le polynôme par $X - \alpha$ où α est une racine). Donc G n'a pas plus de r éléments.
Or, d'après la question précédente, il existe un $c \in G$ d'ordre exactement r, donc c admet r puissances distinctes, donc le groupe engendré par c n'est autre que G tout entier, c'est-à-dire G est cyclique. Ce résultat s'applique, en particulier, au groupe F^* des inversibles du corps.

6. Le groupe $\mathbf{K}_{13}^*$ est, d'après la question précédente, isomorphe au groupe cyclique à $169 - 1 = 168$ éléments. Ce groupe a effectivement

$$\varphi(168) = 2^3 \times 3 \times 7 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 48$$

générateurs. On les trouvera comme produit des éléments d'ordre 3, 7 et 8 qui sont respectivement au nombre de 2, 6 et 4 ($\varphi(168) = \varphi(3)\varphi(7)\varphi(8)$).
Cela est plus facile si l'on fait les remarques suivantes :

(a) Il existe un élément d'ordre 3 dans $\mathbf{K}_{13}^*$ (à savoir $(\overline{3}, \overline{0})$: $(\overline{3}, \overline{0})^3 = (\overline{1}, \overline{0})$).

(b) Une racine α de $(\overline{5}, \overline{0})$ est d'ordre 8. En effet, $\alpha^4 = (\overline{5}, \overline{0})^2 = (\overline{25}, \overline{0}) = -(\overline{1}, \overline{0})$ puis $\alpha^8 = (\overline{1}, \overline{0})$.

(c) Reste à trouver comment fabriquer quelqu'un d'ordre 7. Le plus simple est $\beta = (\overline{4}, \overline{4})$. En effet, ses puissances successives sont :

$$\beta^2 = (\overline{5}, \overline{6}),\ \beta^3 = (\overline{10}, \overline{5}),\ \beta^4 = (\overline{10}, \overline{8}),\ \beta^5 = (\overline{5}, \overline{7}),\ \beta^6 = (\overline{4}, \overline{9})\sqrt{5}, \beta^7 = (\overline{1}, \overline{0})$$

On obtient alors tous les éléments d'ordre 168, i.e. les 48 générateurs de $\mathbf{K}_{13}^*$, en faisant

$$\{(\overline{3}, \overline{0}), (\overline{9}, \overline{0})\} \times \{\alpha, \alpha^3, \alpha^5, \alpha^7\} \times \{\beta, \beta^2, \ldots \beta^6\}.$$

●●●●●●●●●●